Incident Management Service Restoration Team Standard Operating Procedure

V2

Table of Contents

List of figures

Purpose

This document provides instruction for Incident Managers to properly manage a Service Restoration Team (SRT) meeting and provide service delivery requirements.

This information is based on IT Service Management (ITSM) best practices, Information Technology Infrastructure Library version three (ITIL v3) principles, and is supported by the Incident Management Process Definition Document (PDD). ITSM is an integrated process approach that enables IT organizations to achieve IT alignment and deliver end-to-end IT services to the internal customer base in an organized, efficient, and consistent manner.

The Incident Management Standard Operating Procedure (SOP) provides specific guidance to the Incident Manager for managing all incidents during an SRT Meeting.

Audience

It is assumed that Incident Managers reading this document have a basic understanding and familiarity of Incident Management concepts, along with the technical expertise required to understand the information provided.

Scope

The following information is described in this document:

- Process Goal
- Process Description
- Objectives
- Incident Manager Process Flow Overview
- Roles and responsibilities
- Process Steps/Activities
- Process Diagrams
- Notification Procedures
- Form Templates
- Glossary
- Appendices

Policy

All DMDC IT Operations Incident Managers shall become familiar with and follow the procedures outlined within this SOP.

Process Purpose

The goal of the Incident Manager SRT process is to restore normal service operations as quickly as possible and minimize the adverse impact on business operations. The SRT is a team comprised of the Incident Manager, Incident Coordinator and the appropriate resolver group gathered together on a conference call to restore disrupted services. 'Normal service operation' is defined as an operational state where services and configuration items (CIs) are performing within their agreed service and operational levels.

Process Description

The Incident Manager SRT process is a methodical and tactical response of major incidents to ensure compliance with both Service Level Agreements and Organizational Level Agreements for our external and internal customers. The SRT is a triage process used to prioritize major incidents and organize response personnel to resolve disruptions or mitigate potential outages to prevent interruption of service delivery. For those issues that require escalation above the first level of support, the Incident Management SRT process provides a repeatable, consistent and standardized way of resolving customer issues.

Process Scope

An Incident Management SRT Meeting includes any major event that either disrupts or has the potential to disrupt a service. The SRT Meeting is initiated when a major incident is reported to the Consolidated Call Center (CCC).

Objectives

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents.
- Increase visibility and communication of incidents to DMDC and IT Operations (ITO) support staff.
- Enhance the business perception of ITO through use of a professional approach in quickly resolving and communicating incidents when they occur.
- Align Incident Management activities and priorities with those of DMDC.
- Maintain user satisfaction with the quality of ITO services.

Incident Manager Roles and Responsibilities

- Carrying out one or more activities of processes dictated in this document.
- Understanding how their role contributes to the overall delivery of service and creation of value for the business.

- Working with other stakeholders, such as their manager, co-workers, users and customers, to ensure that their contributions are effective.
- Ensuring that inputs, outputs, and interfaces for their activities are correct
- Creating or updating records to show that activities have been carried out correctly.
- Recording incidents.
- Routing incidents to support specialist groups when needed.
- Analyzing for correct prioritization, classification and providing initial support.
- Providing ownership, monitoring, tracking and communication of incidents.
- Providing resolution and recovery of incidents not assigned to support specialist groups.
- Closing incidents.
- Monitoring the status and progress towards resolution of assigned incidents.
- Keeping users and the service desk informed about incident progress.
- Escalating incidents as necessary per established escalation policies.

Supporting Roles for an Incident Management SRT Meeting

Role	Responsibilities
Initial Responder	An Initial Responder can be any member of DMDC or ITO who is informed of or determines that an incident has occurred. Anyone can be the Initial Responder as the Service Desk or Service Operations Center (SOC) team may not always be the first contact person for an Incident and therefore the DMDC ITO Incident Management process defines the role of the Initial Responder. The Initial Responder is anyone in ITO who becomes aware of a particular incident and they are responsible for initiating the process for the logging and support of the incident.
Ticket Owner	Generally, the Ticket Owner is the person in the ITO Service Desk, ITO technical team or the ITO SOC that is responsible of ensuring the incident ticket is created, updated and correctly closed when the incident has been resolved. • The Ticket Owner is the person responsible for each Incident being logged into an Incident Ticket, and each ticket will be assigned an Incident Owner; the Ticket Owner along with the Incident Owner are responsible for ensuring that the incident ticket is updated throughout the lifecycle of the incident.

Role	Responsibilities
	• The Ticket Owner will ensure the end user is informed about the progress being made in resolving the incident. • Where it is believed that progress in resolving an incident has stalled, the Ticket Owner has the responsibility to engage the Incident Owner and, if necessary, escalate the incident to their supervisor. • The method for achieving these requirements is documented within the relevant procedural documentation for the Incident Management process.
Incident Owner	The Incident Owner is the person most responsible for ensuring that the incident is resolved. The Incident Owner is assumed by the person assigned to restore the service being impacted by the incident. If the Incident Owner must pass the responsibility on to another person, this must be done officially and the person being assigned must actively acknowledge they have been assigned as the Incident Owner. For the Incident Owner, the Incident Investigation and Diagnosis stage is the most complex activity of the Incident lifecycle. It is incumbent on the Incident Owner to consider related incidents, known errors, other technical experts, and/or specialist knowledge found in the knowledge database in order to restore the impacted service and resolve the incident. Where it is believed that progress in resolving an incident has stalled, the Incident Owner has the responsibility and authority to pursue and, if necessary, escalate the incident to ensure that resolution is achieved within service targets.
Incident Manager	The Incident Manager is the person most responsible for the oversight of the Incident Management procedures and support aspects during a Major Incident. Key activities include: • Driving the efficiency and effectiveness of the Incident Management process and Major Incident procedures.

Role	Responsibilities
	• Managing the effort of all support staff during the incident restoration and resolution effort. • Producing Incident reports for management during the course of the incident • Provide a documented summary following a Major Incident • Evaluating the effectiveness of the Incident Management process and making recommendations for improvement.
Resolver Group(s)	The Resolver Group represents either the next level of the same support team, or a previously identified specialty support team that will continue the effort towards resolving incidents and service requests that initial support teams or individuals cannot resolve themselves. Support teams in DMDC ITO generally follow a tiered "next level" structure for both internal and external escalations. In this document, escalations are represented as 'Resolver Group escalations' (to other application-oriented or infrastructure-oriented teams). The Resolver Group(s) may include a wide range of IT teams, including: support and applications development personnel, other service management functions, service providers, and other third parties (Oracle, Microsoft, etc.).
Service Owner	The Service Owner is the person within DMDC that is accountable and responsible (per RACI) for a service. While it may be a team or group that is, in effect, the representative of their service, there is one person within the organization who will be "accountable" for the overall decision making and management of each service.
DMDC ITO SOC	The DMDC ITO SOC is usually the first point of contact for the DMDC CCC when reporting a major incident. The SOC is the incident owner for all Priority 1 (refer to Appendix C) incidents in production regardless of the amount of time required to resolve the incident. In the ITO Incident Management process, this role it titled Incident Owner to distinguish between the role that is monitoring the progress (Case Owner) and the role/person who is currently responsible for resolving

Role	Responsibilities
	the incident (Incident Owner).

Incident Manager Process Flow Overview

Currently, the Incident Management process is comprised of three parts beginning with the CCC, Incident Management and Problem Management. The Incident Management process flow diagram below dictates the Incident Management process flow including the relationships with the CCC and Problem management for a holistic view of how a major incident travels from beginning to end.

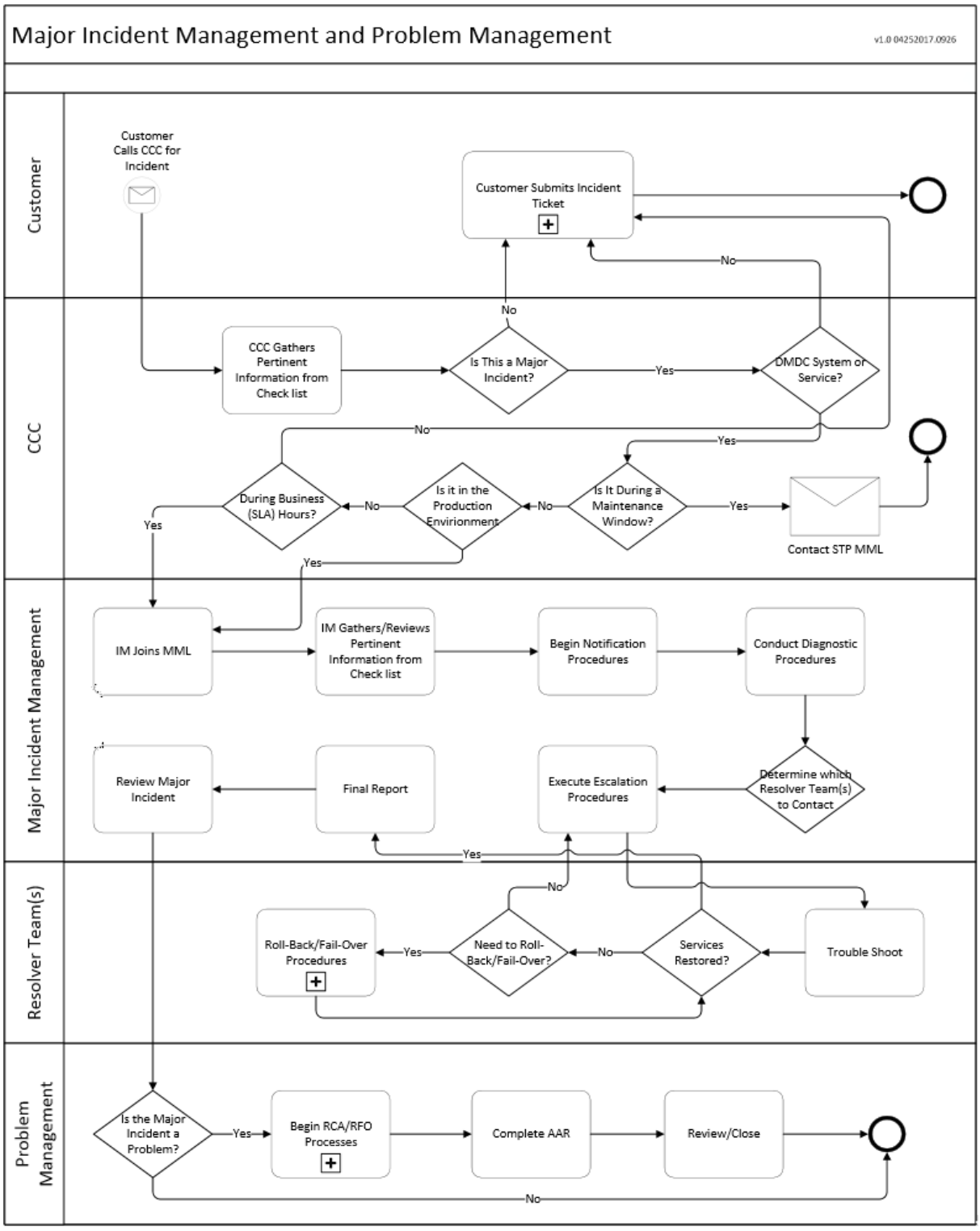

Figure 1 Incident Manager Process Flow Overview

Procedure

Initiating an Incident Manager SRT Meeting

1. The CCC receives a call from a customer stating they have experienced a disruption of service. The CCC discusses the disruption with the customer and presents a series of pre-defined questions to ascertain details necessary to properly triage the disruption and determine the level of assistance required to resolve the issue.

   CCC Disruption Triage Questionnaire

   a. What is the customer's first and last name?
   b. When did the Incident First Occur?
   c. What is the customer contact information?
   d. What application/services are affected?
   e. What is the Application URL?
   f. What errors were received?
   g. How many users at location are affected?
   h. Is it a broad full/intermittent site outage or specific workstations?
   i. Was the incident as a result of a change during a maintenance window?
   j. The disrupted service is part of which environment?
   k. Give a brief Description of the Disruption.

2. The CCC collects the answers to the triage questions and refers to the DSC CCC Decision Tree to Initiate Service Restoral Team (pictured below) to determine if the disruption is an incident to be entered into the CCC incident management system or initiate an Incident Management SRT Meeting as a major incident.
3. The CCC follows the decision tree to determine if the incident meets the criteria to initiate an SRT meeting.
   - If the aforementioned criteria are not met, the incident is regarded as a level 1 service desk incident and a CCC ticket is created and escalated to the appropriate resolver group. The CCC may not have all the required information to adequately make a decision to initiate an SRT Meeting. In this case, the CCC shall initiate a meeting and transfer the details of the major incident to the Incident Managers to determine the level of support required to resolve the disruption.
4. The CCC assigns an Incident Coordinator and initiates the SRT meeting by contacting the on-call Incident Manager using the schedule located at: http://teamsites.ds.dhra.osd.mil/teams/sts/Lists/Systems_OnCall_Support_Phone_Numbers/OnCall_Support.aspx.

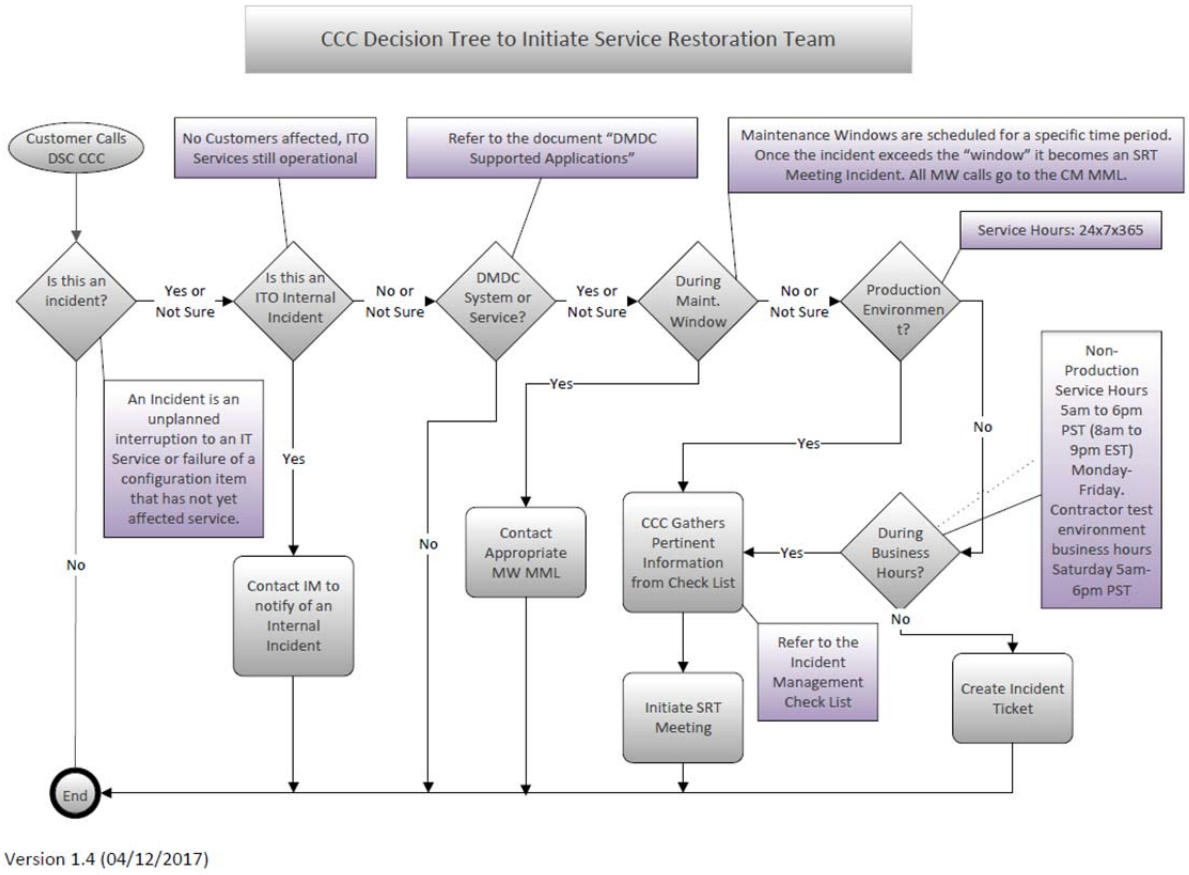

Figure 2 CCC Triage Decision Tree

5. The CCC Incident Coordinator invites the Incident Manager to the Meet Me Line (MML) where all pertinent information regarding the disruption is shared.

Incident Manager's Role during an SRT Meeting

Upon receiving a call from the CCC Incident Coordinator, Incident Managers must obtain as much information about the incident as possible, given the circumstances. In many incident situations, the Incident Manager may need to acquire additional information from the customer or the resolver group that joins the MML.

Incident Manager Steps for an Incident Management SRT Meeting

1. The CCC Incident Coordinator (IC) contacts the Incident Manager and informs the Incident Manager there is an active incident. The IC instructs the Incident Manager to

join the MML and provides details acquired from the customer, stating there is an active major incident.

2. The Incident Manager joins the MML and completes as much of the SRT Incident Manager Check list (refer to Incident Management SRT Check List section) as possible.
3. The Incident Manager determines the impact, urgency, and severity of the incident (refer to Appendix C for a description of impact and urgency levels and to determine the severity level).
4. The Incident Manager begins the appropriate notification procedures (refer to Incident Management SRT Notification Procedures section).
5. The Incident Manager reviews the details provided by the IC and begins collecting the diagnostic analysis information (refer to Incident Management SRT Diagnostic Analysis section).
6. The Incident Manager determines which resolver group shall be called to provide assistance with the reported disruption (refer to the resolver group schedule/list: http://teamsites.ds.dhra.osd.mil/teams/sts/Lists/Systems_OnCall_Support_Phone_Numbers/OnCall_Support.aspx/).
7. The Incident Manager provides the IC with the required resolver group needed for support and requests the CCC have the resolver group join the MML.
8. The Incident Manager informs the resolver group of all the information acquired from the customer and diagnostic analysis.
9. The SRT members troubleshoot the incident until:
    a. Services are restored
    b. A work-around is implemented
    c. The issue is escalated to an external support organization if it is determined the service is not supported by DMDC.
10. The Incident Manager closes the incident and completes the final report (refer to Incident Management SRT Final Report section).
11. The Incident Manager completes the SRT Tracking Worksheet with the pertinent details (see SRT Tracking Worksheet SOP).
12. The Incident Manager reviews the major incident to be considered for entry into the Problem Management process IAW DMDC ITO Problem Mgmt PDD v1-1.

Response Time to a Major Incident: Meeting AQL 14

The Major Incident Team manager's (IM) absolute first step when responding to a major incident is to immediately join the Customer Contact Center (CCC) Meet Me Line (MML). Our FASA contract specifically states administrators are required to join the MML within ten minutes to join MML when the CCC makes initial contact with an Incident Manager Team member and within fifteen minutes to meet

the AQL requirement. It is imperative the IM joins the MML as soon as possible to stop the clock. When the CCC contacts the on-call IM, it is not necessary to discuss the major incident. A quick notification from the event such as: "Customer reports 404 error when accessing the PARS application, you are requested to join the MML," is sufficient. If the primary or secondary IM on-call, without any technical difficulties, does not join the MML within the fifteen minute window from initial contact, the AQL is considered missed.

Note: The fifteen minute clock begins with whomever the CCC makes verbal contact with first. The official recorded response time for IM's is the CCC's first callout time subtracted from the time the IM joins the MML (i.e., CCC contacts the MIM 1535 – IM joins MML at 1545 = 10 minute response time).

The following scenarios are provided for guidance:

1. The CCC attempts to contact the on-call IM via a phone call, but the IM does not answer the call.
    a. If the on-call IM does not pick up when contacted by the CCC, the CCC will typically leave a voicemail and then immediately contact the next on-call IM in rotation. The fifteen minute window will not start for the primary because the CCC did not make verbal contact. Once the first contacted on-call IM receives the recorded message, he/she will join the MML and relieve the other on-call IM.
        i. The primary should not take this as permission to screen calls, as doing so constitutes job abandonment and can lead to disciplinary action.
2. The CCC contacts the primary on-call and the primary answers the call, but circumstances preclude him/her immediate access to a computer or remote access.
    a. If the primary on-call answers a call from the CCC, but is unable to immediately access a computer for remote access, there are several options he/she can take based on the circumstances.
    b. Driving: The on-call IM will tell the CCC that he/she is driving and cannot effectively respond to the call. The primary shall tell the CCC to contact the next on-call team member until he/she can arrive home. The AQL clock begins when the initial on-call IM answered the call. The total response time is a combination of both response times. Once the on-call IM arrives at his/her destination, he/she will join the MML and relieve the other team member on the call.
    c. No access to a computer: If the on-call IM does not have immediate access to a computer for remote access, but is able to join the call without distraction, the IM shall join the MML and explain to the CCC's Incident Coordinator that he/she does not have immediate access to a computer for triage, troubleshooting or taking notes. The primary shall handle the call as effectively as possible. Once the on-call has access to a computer, he/she will inform the IC. Under unique circumstances, the on-call person can still manage the major incident without access to a computer.
3. The CCC contacts the on-call IM, but joining the MML is difficult due to due to telephone technical difficulties at the CCC.

a. It is imperative for an IM to record the times he/she attempted to contact the CCC. If attempts prove unsuccessful after twenty minutes, call the CCC using the number he/she was initially called. Acquire the current status and recommend a CCC bridge line or one of the IM's MMLs to begin the major incident conference call… if appropriate.

Incident Management SRT Check List

Below are typical questions the Incident Manager requires to manage an incident during a Service Restoral Team meeting. See Appendix A for the complete Incident Management SRT Check List Template.

1. What is the Impact Level?
    a. Impact levels 1 thru 5. Relates to the impact on the customer - the extent (depth and breadth) to which the incident impact was felt, and/or the level of customer being affected by the problem.
        - Impact 1: Complete Service Outage
        - Impact 2: Multiple business units and/or regions affected
        - Impact 3: Multiple customers from multiple business units are affected. Some business units or regions are able to work.
        - Impact 4: Multiple customers from a single business unit.
        - Impact 5: Single or no customers have service.
2. What is the Urgency Level?
    a. Urgency levels 1 thru 5. Relates to the importance of the service or environment that is disrupted.
        - Urgency 1: MEC, RAPIDS, PDR, ADR, RBS, BBS, CCEA, CCDDUTA, CCDTIA, CAC, CUF
        - Urgency 2: Applications in Production not in the Urgency 1 list
        - Urgency 3: DEMO1, DEMO2, SILVER DEMO, GOLD DEMO (During Business Hours)
        - Urgency 4: STRESS, MODL OFFICE, 1 MODL OFFICE2 (During Business Hours)
        - Urgency 5: TEST1, TEST2 (During Business Hours)

3. What is the Severity Level?
    a. Severity levels 1 thru 4 defines the type of response and is only applied to Priority 1 incidents:
        - Severity 1: 24x7 Services in Production environment
        - Severity 2: Non 24x7 Services in Production environment

- Severity 3: Lower Region environments
- Severity 4: 24x7 no customers affected

4. What is the Date and Time the Incident Began?
    a. Provided by customer, when the customer first realized there was an outage.
5. When did the Incident First Occur?
    a. The Date/Time the outage actually took place.
6. When was the First Alert?
    a. When the customer called into the CCC to report an outage.
7. When was the First Call?
    a. The Date/Time the CCC contacted the Incident Coordinator.
8. What is the Date and Time the Incident Ended?
    a. The Date/Time when the service was restored or a work-around put in place.
9. Who is the Incident Coordinator?
10. Who is the Incident Manager?
11. What is the customer's first and last name?
12. What is the customer contact information?
13. What application/service is affected?
    a. State the specific service that is experiencing the outage. Do not list related services or dependencies.
14. What errors were received?
    a. Provide a complete list of error codes and related phrases or description.
15. What services are affected by the disruption?
    a. Provide a list of all services affected by the outage including related services or services with dependencies.
16. What is the Application URL?
17. Give a brief Description of the Disruption.
    a. State the description in such a way that it is clear, concise and contains enough detail for other resolver teams to understand.
18. Which environment has the disruption? (For ex. Seaside PROD, Contractor test demo 2...)
19. What is the length of the disruption? (Time of 1st outage)
    a. Provide the length of the outage beginning when the CCC received the call until the service is restored.
20. Is it a broad full/intermittent site outage or specific workstations? (gather workstation ID's if pertinent).
21. How many users at location are affected? (% or #)

   a. This number is used to identify impact of the outage, for example 10% of all customers are unable to use the service.
22. How many other sites and users are affected? (If applicable)
   a. The purpose of the question is to determine how wide spread the outage is affecting customers.
23. Was the incident caused by a change, release or modification to the affected environment(s)?
   a. Determine if the outage was related to a change during a scheduled or un-scheduled maintenance window.
24. If so, what are the CR numbers(s)?
25. Who was the person making the change?
   a. Do not refer to the change request. It is necessary to identify the person who made the change in the case the person is required to join the MML.
26. What were the targeted service, environment and/or systems for change?
   a. A service outage may be the result of a change in another area of the environment. Identify what service was changed and how the service with the outage was affected by the change.
27. What are the results of application monitor review?
28. Provide discussion of the restoration process.
   a. If a fail-over or roll-back is considered, provide the procedures and risks.
29. Discuss any follow-up actions.
   a. Provide a list of necessary actions to remove the work-around, stabilize the application, processes to develop and/or investigate as a problem.

Incident Management SRT Diagnostic Analysis

The diagnostic analysis provides the necessary details to determine the cause of the incident and necessary steps for restoration. Having the information in advance of contacting the necessary resolver group facilitates situational awareness and fosters the efficacy of the incident management process.

Each Major Incident Manager upon joining the MML conference call shall use the Diagnostic Analysis template/form in Appendix B and save the results to the folder: \\mercedes\systems_archive\problem management\signed off srt notes\, then choose the appropriate year folder, month folder and eventually the IM personal folder.

Below are the diagnostic tools available for your analysis. See Appendix B for the Diagnostic Analysis template.

1. SolarWinds:
    a. Check CPU utilization, network/packets in/out.
    b. Identify any warnings.
2. Web Inventory Page
    a. Check App Index, App version, MS health, and host resource health.
    b. Look at other apps on the domain.
    c. Check site URL and app report.
3. Look up past Incidents and Change Requests in the ITSM tool that encompasses the same application(s) and issues.
    a. Identify the root cause and resolution of the tickets.
4. Use a combination of Short Term Planning Notes and deployment spreadsheets, Change Requests, and the Change Calendar to see if changes are responsible or contributed to the incident.

Incident Management Meet Me Line Relief Procedures

How to Transfer a Major Incident from one MIM to Another During a Major Incident MML

From time to time it is necessary to replace MIM on the MML during a major incident. To ensure a quick, efficient transfer of information and responsibility to the MIM relief, it is imperative to standardize the process.

Depending on the circumstances, there is not always a lot of time for an in-depth conversation for absolute situational awareness to the level experienced by the original MIM. However, a standardize process will ensure the best chances of passing information required to continue the major incident MML.

Process:

Original MIM:

In preparation for a MIM relief, the original MIM shall complete the following:

1. Announce to the SRT the MIM relief process will begin.
2. Contact the Incident Coordinator and request he/she contacts the next MIM on-call.
3. When the relief MIM calls into the MML, introduce him/her as the relief and state that you need a moment for the relief process.
4. Introduce the people on the MML and explain their role.
5. Pass a summary of the current situation. It is not necessary to explain all the details from the beginning. The relief only needs to know what is required to continue the SRT meeting.
6. Pass all pertinent information regarding future actions and plans

7. Ask the SRT to provide additional information to fill in the gaps.
8. When all pertinent information is passed, ask the relief MIM if he/she is ready to assume the duties of Major Incident Manager.
9. If accepted, inform the new MIM to expect notes via email. At a minimum, the notes shall include:
    a. Names and roles of resolver groups
    b. Who did what and when
    c. Time stamps

New MIM:

1. Join the call with enough time to get background before transition.
2. Ask any clarifying questions necessary to ensure smooth transition.
3. Accept the MIM Role, and advise the Incident Coordinator.
4. Take notes which overlap with original MIM's notes.

Note: All MIMs have unique ways of recording calls, which is acceptable. However, if you are handing your notes off to another MIM, include ONLY the notes from that call, and ensure they are complete and accurate. Also ensure that the summary included while sending the notes is descriptive enough for the new MIM to reference should the need arise.

Example: (This call happened in July, there was no hand-off, so this is based loosely on true events)

Summary (in email with notes to new MIM):

TSA Secure flight called in stating no records have returned since 1800 last night. TSA has their management and network teams on the line. Networking team and BBS dev are on the line from DMDC. So far, packet captures have indicated missing certificates, so teams are investigating breakdown. Pat Cahill requested CCC reach out to DISA for investigation on their end, and they should be joining soon. DBAs verified health and functionality of databases; they found no errors or warnings. My notes are attached for your reference.

<Attach notes>

On the line:

"This is Morgan, I am going to start the relief process for a new Incident Manager. Andrew, please contact the next available Incident Manager to join the MML."

"Jerry Jones has joined the Meet Me Line"

"Hi Jerry, this is Morgan, are you ready for the brief?"

"Yes"

"To everyone on the line, Jerry Jones is going to relieve me as Incident Manager, please stand-by while I give a quick brief. "Jerry, we have Bonaventure and Marco on the line from TSA, as well as various people from their team (would try to name everyone, but in this call, they had 10+ people). From DMDC, we have Paul and Mark from networking, as well as Matt from BBS. DBAs have confirmed successful and healthy databases; web team confirmed healthy nodes and deployments. CCC is currently reaching out to DISA for investigation on their end, as both TSA and DMDC agree the outage is caused by mismatched certs. TSA network travels through external firewalls before reaching us, so I would recommend contacting those companies, as well. Does anyone on the line have anything to pass to Jerry?"

"Jerry, do you have any questions?"

"Nope, thanks Morgan. CCC, I am taking over from here."

"OK. Thanks Jerry, I will send you my notes now. CCC, I am taking off, Jerry is now your MIM. Please send us both the final notes."

Incident Management SRT Notification Procedures

1. Contact the following for all MEC or SEV-1 incidents via text message:
   a. (b) (6) [redacted]
   b. (b) (6) [redacted]

   Use the following message:

   "This is the IM Team: FYI, there is a MEC **(or name of service)** incident that just started. The impact is **(how many are affected)**. What we know is (brief description). We are tracking it and will keep you informed."

2. Continue with text messages every 30 minutes after the initial contact if more information is known.
3. Prior to contacting the resolver group, the Incident Manager shall have the Incident Manager SRT Diagnostic Check List complete and available.

Incident Management SRT Escalation Procedures

Escalation procedures ensure the appropriate personnel and resources are available to troubleshoot the root cause analysis. Occasionally, it is necessary to obtain additional resources

or contact senior level personnel to assist in a disruption when the current level of expertise cannot determine the root cause. Below are guidelines to use when escalating a disruption:

1. During an outage, the Incident Manager completes the diagnostic process to determine which resolver group is required to begin the root cause analysis. Typically, the Incident Manager contacts one or more of the following during the initial stages of troubleshooting:
    a. The customer that reported the disruption
    b. The owner of the service
    c. On-call Systems Database Administrator
    d. On-call Application Database Administrator
    e. On-call Network Administrator
    f. On-call Windows Administrator
    g. On-call Unix/Linus Administrator
    h. The person that conducted the last change or deployment of the service
2. During the troubleshooting stage, any member of the SRT may recommend escalation to another resolver group, depending on the evidence found, to assist with determining the root cause.
3. Any time the Incident Manager believes the circumstances are beyond the ability of any the team members, the Incident Manager may request additional personnel of one or more of the resolver groups on the call. It is possible that other resolver group members have more technical expertise for that particular situation.
4. The Incident Manager may escalate the technical expertise to the resolver group team lead when that level of expertise is required.
5. The Incident Manager may escalate the technical expertise to the resolver group branch chief when that level of expertise is required.
6. Occasionally, the situation may be so severe that escalation to senior leadership is required. This is a decision in which the Incident Manager will have to use their best judgement. A few situations that may require escalation to senior leadership:
    a. The service disruption cannot be restored
    b. The service disruption will require more than 1 workday to restore
    c. The service disruption requires a decision at the level of the senior leadership
    d. The service disruption continues for over 4 hours and root cause has not been determined

Roll-Back, Disaster Recovery Procedures

In rare instances, if the root cause cannot be determined or there is no means to restore the service, a roll-back or fall-over via disaster recovery may be considered. Use the following guidance:

A. **Roll-back**: Typically, a roll-back is used only when there was a recent change or deployment. During a scheduled maintenance window, there are many changes, patches, and deployments occurring. Following a change, patch, or deployment, quality assurance personnel ensure all services are restored and functioning within normal limits.

B. The following general rules apply during a maintenance window:

1. Verification of normal operations is required within 30 minutes of completing the change, patch, or deployment.
2. Failure to verify normal operations may result in one or more of the follow actions:
    a. Immediate roll-back to a previous version
    b. Additional scrutiny of future deployments for the Project Team
    c. An SRT meeting will be initiated if verification exceeds the maintenance window

C. The following general rules apply during non-maintenance window:

1. If no progress is made for 30 minutes after all efforts were attempted, the Incident Manager discusses rolling back the change, patch, or deployment with the members of the SRT.
2. When a consensus is reached to roll-back or the Incident Manager believes it is required to restore services (even when it contradicts members of the SRT), he/she will advise senior leadership and recommend a roll-back to the last known good status.
3. Senior leadership will be made aware of roll-back procedures in accordance with roll-back procedures as dictated in the change request.

D. **Disaster Recovery**: When it is determined the roll-back process did not restore services or there is no recent restore point, disaster recovery is an appropriate fall-over option.

1. When a consensus or the Incident Manager determines it is necessary to execute a fail over to restore services (even when it contradicts members of the SRT), he/she advises senior leadership and recommends a fail-back to systems on hot standby.
2. Senior leadership is made aware of the fail-back procedures in accordance with Disaster Recovery policy and process.

Emergency Change Procedure

During the course of the restoration process of the incident, it may be necessary to implement an Emergency Change Request to restore services.

An emergency change must first be officially classified as an “emergency” and that includes meeting certain criteria and very specific requirements detailed in the Change Management policy and process.

In situations where the Emergency Change can be implemented before the Emergency Change Request (ECR) is written, verbal approval must be received by ITOps Senior Management.

The CR Requestor must note the verbal approval is received by inserting the Approval Authority name in the “Approving Authority” field before the ECR is submitted. Additionally and as the ECR must be created and submitted within 4 hours following the implementation of the change and/or the recovery of the service regardless of the day of week or time of day of the emergency change.

With the ERC being submitted after-the-fact, the TRB and CCB review will occur after the change is made. Each ECR submitted will also be reviewed by the ITOps Director or Deputy Directory.

Fields to be completed in Emergency Change Request

The following fields shown in Table 1 must be completed within the ECR:

Table 1: Change Request Requested Information

Field	Description
Requestor	The name of the Requestor
Affected End User	The name of the Affected End User is generally the Service Owner or the Key Stakeholder of the service being impacted and requiring the ECR
Category	CR.*division_name* --- In this field, select/enter the Division that owns the service that the change is being applied to. Examples include: CR.SYSTEMS, CR.DEERS, CR.ES, CR.IS, etc.
Approving Authority	All Emergency Changes must have a senior manager approve the change; ideally this would be the Division Director, Service Owner or other senior manager that can provide the assurance that the risk of implementing change is less than the risk of not performing the change. See the section on Authorized Emergency Change Approvers below
Status	Leave as "Submit" - Once the Change Request is saved, it will be automatically forwarded to your Division Approval Authority. Change to "Draft" - If you plan on making further changes to the Change Request after you save it, change the status to "Draft" before you save it. Once you have finalized the Change Request, change the status back to

Field	Description
	"Submit."
Priority	**Emergency:** Immediate or Work has already been completed or must be completed immediately to restore a failed service. **Critical:** Best Effort (Same day or within 1 business day)
Need by Date	The Need-by-Date is the date the Emergency change was performed.
Implementation Date	Is the date and time the Emergency Change was performed. Note: In some cases this date cannot be entered until after the ECR is approved; as necessary, this will need to be entered by the Change Manager or team lead at the time the CR is set to "Ready to Close"
Order Summary	One line summary of the Change Request.
Order Description	In situations where an emergency change was required, there should be ample details to support the need for an emergency and of all the work performed. Include the following information if it is applicable to your Emergency Change: • Date and Time of the Emergency Change – put the actual date & time at the top of the description field • What exactly was the incident/issue that was experienced and that the change was to correct? • Specific details relating to the end result/outcome of the change (more than one word "Change Success". • By name and contact phone number who actually performed the change and if there were others involved • Detailed List of Steps: If known, provide a list of configuration steps that need to occur.
Properties Tab	Fill out the appropriate fields when applicable.
Configuration Item Tab	Attach any Configuration Items that are associated with the Change Request. Select the Update CIs ($) button within the tab.
Related Orders	Attach a related Parent Change Order
Incidents / Problems	Emergency Changes are generally associated with an SRT. Identify the SRT number in the Description field. If there is any related Requests, Incidents, or Problems, be sure to

Field	Description
	identify them here.
Cost/Plans Tab	The following fields are REQUIRED. Provide a detailed explanation for each requirement. o Business Case o Implementation Plan o Backout Plan
Attachments Tab	Attach any documents that are relevant to the Change Request.

Important Fields for an Emergency Change Request

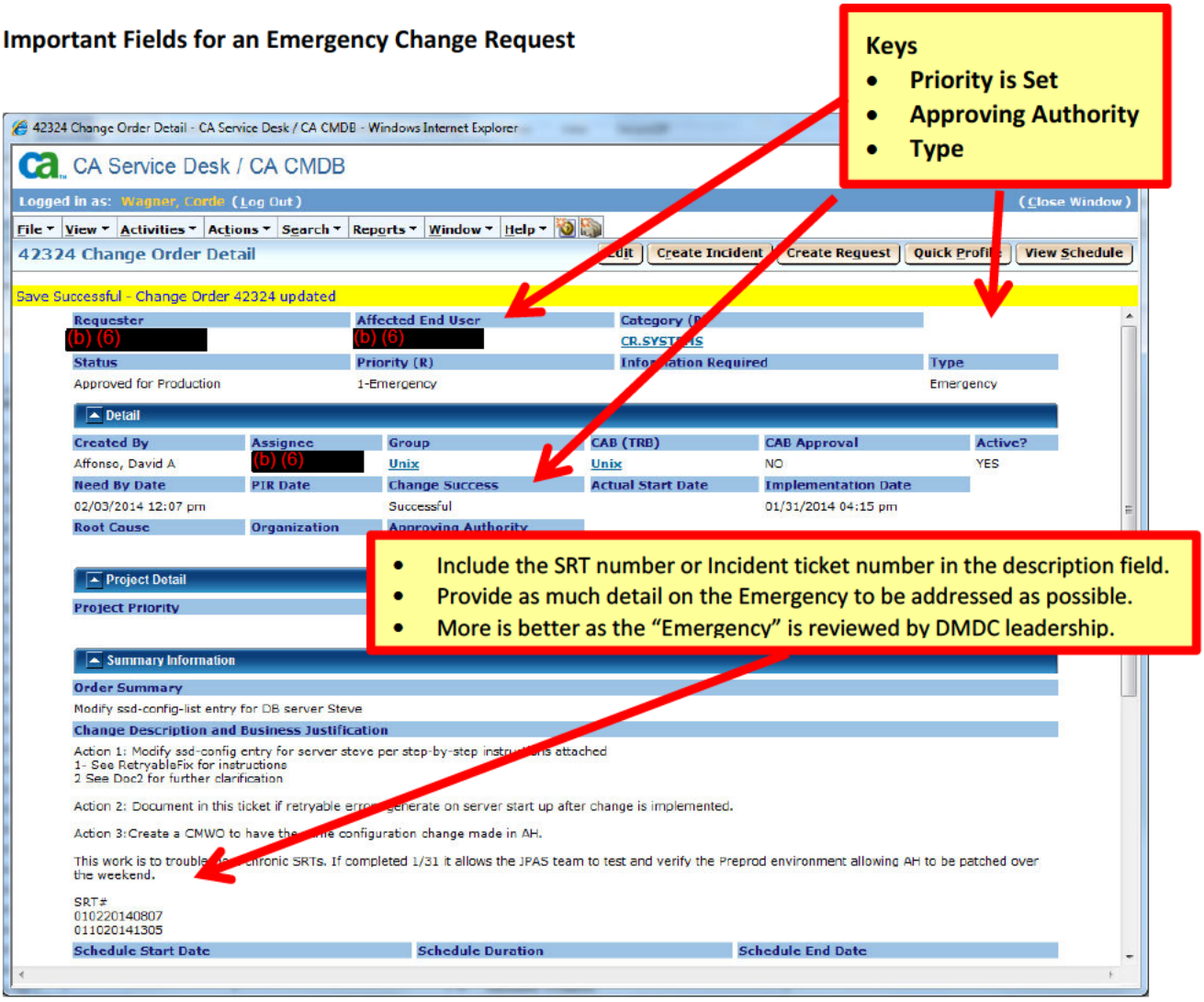

Figure 3 Emergency Change Request

Authorized Emergency Change Approvers

All changes to the production environment must be documented via a change request, which must be approved before the change can be executed. With very few exceptions, and where a verbal approval is given by an approved ECAB member, approvals after the change has been executed are not permitted.

- Prior to the Emergency Change, the implementer needs to obtain verbal approval from either the change Team Lead AND (b) (6), or the Team Lead and 2 other ECAB members.
- The ECAB is comprised of (b) (6), and the ITOps Team leads.

- In situations where a DMDC application or service that is owned by division other than ITOps, the requester may obtain approval from the Division Director or other senior manager within the Division. Should they not be available, a ITOps Division ECAB or ECR approver can be the Authorized Approver. In either of these situations, the person submitting the ECR should provide details of the authorization as necessary.

For ITOps, a Service Recovery change may be executed with *prior* approval of a designated Emergency Change Approver approvers identified in the following table.

Feature	Environment	Approver Name - Role
Unix	• Production • CT	• (b) (6) – Director, ITOps • (b) (6) – Deputy Director, ITOps • (b) (6) • (b) (6)
Windows	• Production • CT	• (b) (6) – Director, ITOps • (b) (6) – Deputy Director, ITOps • (b) (6)
Network	• Production • CT	• (b) (6) – Director, ITOps • (b) (6) – Deputy Director, ITOps • (b) (6)
Web	• Production • CT	• (b) (6) – Director, ITOps • (b) (6) – Deputy Director, ITOps • (b) (6)
Oracle / Database	• Production • CT	• (b) (6) Director, ITOps • (b) (6) – Deputy Director, ITOps • (b) (6) • (b) (6)
Storage	• Production • CT	• (b) (6) – Director, ITOps • (b) (6) – Deputy Director, ITOps • (b) (6)
IAB	All	• (b) (6) • (b) (6) • (b) (6) – Deputy Director, ITOps
DMDC Applications not "Owned" by IT	All	Per the list on the Approving Authorities page

Post Emergency Change CR Review Steps

When processing an Emergency Change Request (ECR) for post-implementation approval, a good practice is to have the TRB and the CCB review what was done by the ECR.
After the implementation of an Emergency Change, the change implementer is “Responsible” for submitting the Emergency Change Request (ECR) within 2 hours following the completion of the emergency change. Note: If agreed to by the Change Implementer, the Change Requester or other designee can submit the ECR, but the “responsibility” remains with the Change Implementer).

Additional guidance for reviewing and processing ECRs post-implementation:

- An Emergency CR must be entered into USD and submitted for review no later than 4 hours after the implementation.
- The ECR will be processed like any other Normal change request, but going through the same review steps.
- If the TRB and/or the CCB disagree with any part of the change then the TRB & CCB would work together to decide upon if any other work is necessary, if the EC should be "disapproved" and backed-out.
- If the TRB and/or CCB reviewers identify that any part of the EC included a process or procedure issue, identify what the issue is, make any recommendations to resolve the situation, process or procedure, and please let the Change Manager know.
- If in working through the review a “Problem” (by ITIL definition), please let the Problem Manager know so they can add the identified problem into the Problem Register.

Incident Management SRT Final Report

After an SRT MML, the Incident Manager:

1. Provides a completed Incident Manager Checklist with details regarding the restoration, root cause, and follow-up action items.
2. Sends the completed check list with final notes to the DSC CCC.
    a. DSC compiles the information and sends it by email to the DODHRA BEAU-ALEX DMDC List Customer Incident distribution list.
    b. Ensures the information in this email is accurate and sufficient for an external stakeholder (senior management, government oversight, application owners, and etc.) to have a general understanding of what took place throughout the incident.
3. Use the following guidance when filling out the final report:
    a. Do not allow the pace of the SRT meeting to outpace your ability to take notes and understand the details of what is taking place.

b. Ensure you have a good understanding of what is taking place. As questions as necessary such as; who, what, how and why.
c. Your situational awareness should reach a point where you can easily explain in simple terms the situation and nuances.
d. Review the notes provided by the CCC IC. Make corrections and additions as necessary to explain the situation. Realize that other IT Ops teams read the notes.
e. Ensure the details are added to the SRT Tracking worksheet. If a follow-up is required, ensure it is handled on time.

Continual Process Improvement

Recommendations for the improvement of this SOP should be submitted to the DMDC IT Operations Incident Manager lead.

Document History

This DMDC Incident Management Process document supersedes any previously published incident management process or procedure.

Version	Activity	Date	Author
V2	Updated Version	24 Feb 2017	(b) (6)
V2	Updated Final Reports procedures	14 Apr 2017	
V2	Updated policy regarding diagnostic analysis	27 Apr 2017	
V2	Updated Priority and Severity Matrix	01 May 2017	
V2	Add CCC, IM & PM Process Flow	02 May 2017	
V2	Added Emergency Change Procedures	05 May 2017	
V2	Removed any reference to Internal Incident	09 Sep 2017	
V2	Removed any reference to TeamQuest	09 Sep 2017	
V2	Add Incident Management Meet Me Line Relief Procedures	12 Dec 2017	

References

- DoD IT Service Management Instruction 8440.01
- DMDC IT Operations Incident Management Process Definition Document, February 2017
- ITIL Service Operation, TSO, 2011

Appendix A Incident Management SRT Check List/Final Report

Incident Management SRT Check List/Final Report				
	Impact Level		First Occurred	
	Urgency Level		First Alert	
	Severity Level		First Call	
	Date/Time Incident Began:		Date/Time Incident Ended:	
1	Incident Coordinator:			
2	Incident Manager:			
3	Customer First and Last Name:			
4	Customer Contact Information:			
5	What application(s)/service(s) are affected?			
6	What errors were received?			
7	What services are affected by the disruption?			
8	Application URL:			
9	Brief Description of Disruption:			
10	Which Environment is affected? (For ex. Seaside PROD, Contractor test demo 2...)			
11	Length of disruption? (Time of 1st outage)			
12	Is it a broad full/intermittent site outage or specific workstations (gather workstation ID's)			
13	How many users at location are affected? (% or #)			
14	How many other sites and users are affected? (If applicable)			
15	Was the Incident caused by a change, release or modification to the affected environment(s)?			
16	If so, what is the CR Number(s)	17	Person making the change	

Incident Management SRT Check List/Final Report	
18	Targeted service, environment and/or systems for change?
19	Results of application monitor review?
20	Discuss restoration process:
21	Discuss follow-up actions:

Appendix B Incident Management SRT Diagnostic Check List

Incident Management SRT Diagnostic Check List

1.	SolarWinds:
a.	a. Check CPU utilization, network/packets in/out
b.	b. Identify any warnings

2.	Web Inventory Page
a.	a. Check App Index, App version, MS health, and host resource health
b.	b. Look at other apps on the domain
a.	c. Check site URL and app report

3.	Look up past Incidents and Change orders in CMDB that encompass the same application(s) and issues.
a.	a. Identify what was the cause and restoration in these tickets

4.	5. Use a combination of Short Term Planning Notes and deployment spreadsheets, Change Orders, and Change calendar to see if changes could be responsible or contribute to the incident.

Appendix C Priority and Severity Matrix

Using the following Priority and Severity Matrix, the Incident Manager will determine the impact, urgency and severity of a major incident.

Major Incident	Severity Matrix For Major Incidents				Impact				
					Complete Service Outage 100%	Multiple business units and/or geographical regions affected or >60% but <100% of all customers	Multiple business units and/or geographical regions affected or >30% but <60% of all customers	Multiple business units and/or geographical regions affected, single site or >0% but <30% of all customers	No Customers Affected or during non-business hours
	Priority 1	Urgency	Tier 0, 1 (Claims, 24x7)	MEC, RAPIDS, PDR, ADR, RBS, BBS, CCEA, CCDDUTA, CCDTIA, CAC, CUF	Severity 1	Severity 1	Severity 1	Severity 1	Severity 2
			Tier 2 (Production)	Applications in Production not in the Tier 1 list	Severity 2	Severity 2	Severity 2	Severity 2	Severity 3
			Tier 3 (Contractor Test)	DEMO1, DEMO2, SILVER DEMO, GOLD DEMO (During Business Hours)	Severity 3	Severity 3	Severity 3	Severity 3	Severity 4
			Tier 4 (Stress, MODL & Test)	STRESS, MODL OFFICE, 1 MODL OFFICE2, TEST1 & TEST2 (During Business Hours)	Severity 4	Severity 4	Severity 4	Severity 4	Severity 5

Severity Level	Required Action
Severity 1	All hands, Immediate Response, Director/Deputy Notified, follow major incident management SOP
Severity 2	Normal Ops, Immediate Response (CCC Notification Procedures), follow major incident management SOP
Severity 3	Normal Ops, Immediate Response During Business Hours, follow major incident management SOP
Severity 4	During Businness Hours if resources are available
Severity 5	Submit incident ticket

Incident	Severity Matrix for Incidents			Impact			
				Any number of customers affected across all sites	Single site or small groups of individuals	Individuals	Response Times (Defined as when a technician acknowledges customer's ticket)
	Priority 2 (High)	Urgency	VIPs, SIPRNet, Operational apps, no access to services: time sensitive	High	High	medium	4 Hours
	Priority 3 (Medium)		NIPRNet, no access to service(s): time sensitive	High	Medium	medium	12 Hours
	Priority 4 (Low)		Intermittent access to service(s): not time sensitive	Medium	Medium	Low	24 Hours